## REMARKS

Applicant requests reconsideration and allowance of the subject patent application in light of the changes above and the remarks that follow.[1] Claims 16-31 are currently pending. Claim 31 has been amended.

### I. Claim Objection

Claim 31 was objected to on the basis of terminology that was considered to be informal. It is believed that the foregoing amendment to claim 31 addresses the Examiner's concern.

### II. Rejection Under 35 U.S.C. § 103(a)

Claims 16-31 were rejected under § 103(a) on the basis of U.S. Publication No. 2002/0069361 to Watanabe et al. (hereinafter "Watanabe") in view of U.S. Publication No. 2001/0036301 to Yamaguchi et al. (hereinafter "Yamaguchi"). The rejection is traversed as follows.

Claim 16 recites a method of securing access to a piece of equipment, the method comprising:

> obtaining a reference datum for an authorized user, wherein said reference datum comprises at least an authentic biometric signature;
> storing an encrypted version of said authentic biometric signature on said piece of equipment;
> acquiring, at a sensor, a plain biometric signature for a user requesting access to said piece of equipment;
> transmitting, from said piece of equipment, said encrypted biometric signature to an authentication medium that is separate from said piece of equipment;

[1] The Office Action contains statements characterizing the claims and related art. Regardless of whether any such statements are specifically addressed herein, Applicant's silence as to these characterizations should not be construed as acceptance of them.

decrypting, in said authentication medium, said encrypted authentic biometric signature received from said piece of equipment;

verifying, in said authentication medium, the authenticity of said plain biometric signature by comparing said plain biometric signature of said user with said decrypted authentic biometric signature of an authorized user; and

granting said user access to said piece of equipment if said comparison is successful and denying access if said comparison fails.

As previously submitted in the Amendment dated January 25, 2010, in the context of the present invention, the biometric signature, e.g. finger print, that is required for access to a piece of equipment, e.g. a computer, is stored on that piece of equipment. By means of such an arrangement, a single authentication medium, e.g. smart card, can be used to authorize access to a variety of different pieces of equipment, without having to store the biometric signatures for all of those pieces of equipment.

Watanabe and Yamaguchi, whether considered individually or in combination, do not disclose a method of securing access to a piece of equipment comprising storing an encrypted version of said authentic biometric signature on said piece of equipment, and transmitting, from said piece of equipment, said encrypted biometric signature to an authentication medium that is separate from said piece of equipment, as recited in claim 16.

Watanabe discloses user authentication using a person identification certificate (IDC) in conjunction with a public key certification (PKC). See paragraph 0158. In Watanabe, the IDC includes template information including finger print information, retina pattern information, iris pattern information, voice print information, and handwriting information, to identify a corresponding person. Watanabe discloses that the IDC, including the template information, is stored after

being encrypted. See Watanabe: paragraphs 0225. The IDC is issued by a person identification certificate authority (IDA), as illustrated in Figs. 9-18 of Watanabe.

Watanabe discloses the following examples of comparing user-entered sampling information (such as finger print information) and the IDC for user authentication. Referring to Fig. 19 of Watanabe, the IDC is stored in the IDA, and a comparison between the sampling information and the IDC is made by the IDA to determine whether access to a User Device (UD) or a Service Provider (SP) is granted.

Referring to Fig. 20 of Watanabe, the IDC is stored in an IC card 450, and a comparison between the sampling information and the IDC is made by the SP or the UD to determine whether access to the SP or the UD is granted.

Referring to Fig. 21A of Watanabe, the IDC is stored in the IDA, and a comparison between the sampling information and the IDC is performed by the UD to determine whether access to the UD is granted.

Referring to Fig. 21B of Watanabe, the IDC is stored in the IDA, and a comparison between the sampling information and the IDC is performed by the SP to determine if access to the SP requested by the UD is granted.

Referring to Fig. 21C of Watanabe, the IDC is stored in the IDA, and a comparison between the sampling information and the IDC is performed by the IDA to determine if access to the SP or the UD is granted.

Referring to Fig. 22 of Watanabe, the IDC is stored in the IDA, and a comparison between the sampling information and the IDC is performed by the UD to determine if access to the UD is granted.

Referring to Fig. 23 of Watanabe, the IDC is stored in the IDA, and a comparison between the sampling information and the IDC is performed by the SP to determine if access to the SP requested by the UD is granted.

Referring to Fig. 24 of Watanabe, the IDC is stored in the UD, and a comparison between the sampling information and the IDC is performed by the UD to determine if access to the UD is granted.

Referring to Figs. 25 and 26 of Watanabe, the IDC is stored in a personal terminal such as an IC card, and a comparison between the sampling information and the IDC is performed by the UD to determine if access to the UD is granted.

Referring to Fig. 27 of Watanabe, the IDC is stored in a personal terminal such as an IC card, and a comparison between the sampling information and the IDC is performed by the personal terminal.

Referring to Figs. 28-30 of Watanabe, the IDC is stored in the UD, and a comparison between the sampling information and the IDC is performed by SP to determine if access to the SP requested the UD is granted.

Referring to Fig. 31 of Watanabe, the IDC is stored in the UD, and a comparison between the sampling information and the IDC is performed by the UD to determine if access to the SP is granted.

As seen from the examples of comparing user-entered sampling information disclosed in Watanabe, the reference does not disclose an example that includes storing IDC in a piece of equipment to which access is requested, and transmitting, from the piece of equipment, the IDC to an authentication medium that is separate from said piece of equipment. Accordingly, Watanabe fails to disclose a method of securing access to a piece of equipment comprising storing an encrypted version of

said authentic biometric signature on said piece of equipment, and transmitting, from said piece of equipment, said encrypted biometric signature to an authentication medium that is separate from said piece of equipment, as recited in claim 16.

It is respectfully submitted that Yamaguchi does not remedy the deficiencies of the Watanabe publication. Yamaguchi discloses that registered finger prints are stored in the storage unit 414 of the finger print checking device 411. Alternatively, the registered finger prints are stored in a hard disk drive 425 of a host computer 420, to be downloaded to the storage unit 414, or in an IC card 431, to be transferred to the finger print checking device 411 through the host computer 420.

In Yamaguchi, the host computer 420 is not the device, or piece of equipment, to which access is being requested. Rather, the host computer 420 serves as a storage device for providing registered finger prints to the finger print checking device. In Yamaguchi, when the finger print checking device 411 determines that a newly presented finger print matches a registered finger print, it controls the unlocking of the entrance/exit system (paragraph 0041). There is no disclosure in Yamaguchi that the finger print checking device operates to provide access to the host computer 420. As such, Yamaguchi does not disclose storing finger prints in a system to which access is requested, and transmitting, from the system, the stored finger prints to the finger print checking device that is separate from the system. Accordingly, Yamaguchi fails to disclose a method of securing access to a piece of equipment comprising storing an encrypted version of said authentic biometric signature on said piece of equipment, and transmitting, from said piece of equipment, said encrypted biometric signature to an authentication medium that is

separate from said piece of equipment, as recited in claim 16. Accordingly, Yamaguchi does not remedy the deficiencies of the Watanabe publication.

In the Office Action, it is asserted that storing an encrypted biometric sample on a computer is obvious because Yamaguchi discloses that more samples can be stored in a computer than an IC card. Such Examiner's proposed reason for combining the references is unsound.

If the reason to modify Watanabe is to store more encrypted biometric samples than an IC card can hold, as proposed by the Examiner, these encrypted biometric samples are likely to be stored in IDA, where the encrypted biometric samples are generated. There is no disclosure in Watanabe that an IDA has a limitation in storage space. With this arrangement, the IC card can efficiently acquire the IDC from the IDA to compare with sampling information.

There are no reasons to modify Watanabe so that the IDC is moved from the IDA to a piece of equipment to which access is requested, and is moved again to the IC card to compare with sampling information, as proposed by the Examiner. In such arrangement, the IDC is moved twice, without gaining any benefits. Accordingly, the reason to modify Watanabe proposed by the Examiner is unsound.

In view of the foregoing, it is respectfully submitted that the Watanabe and Yamaguchi references, whether considered individually or in combination, do not suggest the subject matter of claim 16. For similar reasons, it is respectfully submitted that the references do not suggest the subject matter of independent claims 21 or 26, or any of the claims depending therefrom.

**Conclusion**

For the reasons set forth above, Applicant respectfully requests allowance of claims 16-31.

In the event that there are any questions concerning this paper, or the application in general, the Examiner is respectfully urged to telephone Applicant's undersigned representative so that prosecution of the application may be expedited.

If additional fees are required for any reason, please charge Deposit Account No. 02-4800 the necessary amount.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: June 29, 2010

By: Weiwei Y. Stiltner
Weiwei Y. Stiltner
Registration No. 62979

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620

Customer No. 21839